CLAIMS

1. A copyright protection system comprising: a recording apparatus operable to encrypt a content and to record the encrypted content; a recording medium on which the encrypted content is recorded; and reproduction apparatuses, each of which is operable to read out and decrypt the encrypted content recorded on said recording medium,

wherein said reproduction apparatuses are classified into N-categories, N being a natural number greater than one,

said recording apparatus is operable (a) to generate, for the respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key, (b) to generate the encrypted content which is the content encrypted based on the media key, and (c) to record at least the N-pieces of revocation data and the encrypted content onto said recording medium, the device key data being held by said reproduction apparatuses of the respective N-categories, and the device key being held by a specific reproduction apparatus of the respective categories, and

said reproduction apparatuses are each operable (a) to read out, from said recording medium, revocation data, among the N-pieces of revocation data, which is for the category to which said reproduction apparatus belongs, and the encrypted content, and (b) to decrypt the encrypted content based on the read-out revocation data.

2. The copyright protection system according to Claim 1,

wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatuses of a corresponding category, and

said reproduction apparatuses of the respective categories

are each operable (a) to read out, from said recording medium, the corresponding encrypted media key data and the encrypted content, (b) to obtain the media key by decrypting the encrypted media key data using the held device key, and (c) to decrypt the encrypted content based on the obtained media key.

3. The copyright protection system according to Claim 2,

wherein said recording apparatus is operable to generate an encryption key based on the media key, and to encrypt the content based on the encryption key, and

said reproduction apparatuses of the respective categories are each operable to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key.

4. The copyright protection system according to Claim 2,

wherein said recording apparatus is operable to encrypt the content using a content key, to generate an encrypted content key by encrypting the content key using the media key, and to record the generated encrypted content key onto said recording medium, and

said reproduction apparatuses of the respective categories are each operable to read out the encrypted content key from said recording medium, to obtain the content key by decrypting the encrypted content key using the media key, and to decrypt the encrypted content using the obtained content key.

5. The copyright protection system according to Claim 1,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by said reproduction apparatuses of the corresponding category,

said recording apparatus is operable to encrypt the content

using a content key, to generate N-pieces of encrypted content keys by encrypting the content key using N-pieces of media keys, and to record, onto said recording medium, at least the N-pieces of encrypted media key data, the N-pieces of encrypted content keys, and the encrypted content, and

said reproduction apparatuses of the respective categories are each operable (a) to read out, from said recording medium, the encrypted media key data for the corresponding category, the encrypted content key for the corresponding category, and the encrypted content, (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the held device key, (c) to obtain the content key by decrypting the encrypted content key for the corresponding category using the obtained media key for the corresponding category, and (d) to decrypt the encrypted content using the obtained content key.

6. The copyright protection system according to Claim 1,

wherein said recording apparatuses are made up of:

second reproduction apparatuses belonging to a second category, each of which is operable to read out and decrypt the encrypted content recorded on the recording medium; and

first reproduction apparatuses, each of which includes:

a read-out apparatus of the second category operable to read out and perform a part of a decryption process on the encrypted content recorded on the recording medium; and

a decryption apparatus of a first category, connected to said read-out apparatus of the second category, operable to perform a part of the decryption process on the encrypted content,

wherein said recording apparatus is operable (a) to generate, based on a media key and on device key data held by said decryption apparatuses of the first category, first revocation data intended for

revoking a device key held by a specific decryption apparatus of the first category, (b) to generate, based on a media key and on device key data held by said apparatuses of the second category, second revocation data intended for revoking a device key held by a specific apparatus of the second category, (c) to generate an encrypted content which is the content encrypted based on the media key, and (d) to record at least the first revocation data, the second revocation data, and the encrypted content onto said recording medium,

said second reproduction apparatuses are each operable to read out the second revocation data and the encrypted content from said recording medium, and to decrypt the encrypted content based on the second revocation data, and

in each of said first reproduction apparatuses:

said read-out apparatus of the second category is operable (a) to read out, from said recording medium, the first revocation data, the second revocation data, and the encrypted content, and (to) supply intermediate data and the first revocation data to said decryption apparatus of the first category; and

said decryption apparatus of the first category is operable to obtain the content by performing the decryption process, based on the first revocation data, on the intermediate data supplied by said read-out apparatus of the second category, the intermediate data being the encrypted data on which the part of the decryption process has been performed based on the second revocation data.

7. A recording apparatus which encrypts a content and records the encrypted content,

wherein said recording apparatus is operable (a) to generate, for respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key, (b) to generate an encrypted content which is the content encrypted based on the media key, and (c) to record at least the N-pieces of

revocation data and the encrypted content onto a recording medium, the device key data being held by reproduction apparatuses classified into N-categories and belonging to the respective categories, the device key being held by a specific reproduction apparatus of the respective categories, and N being a natural number greater than one.

8. The recording apparatus according to Claim 7,

wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by the reproduction apparatuses of a corresponding category.

9. The recording apparatus according to Claim 8,

wherein said recording apparatus generates an encryption key based on the media key, and to encrypt the content based on the encryption key.

10. The recording apparatus according to Claim 8,

wherein said recording apparatus encrypts the content using a content key, generates an encrypted content key which is the content key encrypted using the media key, and records the generated encrypted key onto the recording medium.

11. The recording apparatus according to Claim 7,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by the reproduction apparatuses of the corresponding category, and

said recording apparatus is operable (a) to encrypt the content using a content key, (b) to generate N-pieces of encrypted content keys by encrypting the content key using N-pieces of media

keys, and (c) to record, onto the recording medium, at least the N-pieces of encrypted media key data, the N-pieces of encrypted content keys, and the encrypted content.

12. The recording apparatus according to Claim 7,

wherein said recording apparatus (a) generates, based on a media key and on device key data held by decryption apparatuses of the first category, first revocation data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) generates, based on a media key and on device key data held by apparatuses of the second category, second revocation data intended for revoking a device key held by a specific apparatus of the second category, and (c) generates an encrypted content which is the content encrypted based on the media key, and to record at least the first revocation data, the second revocation data, and the encrypted content onto the recording medium.

13. A recording medium on which a content is recorded,

wherein on said recording medium, at least revocation data and an encrypted content are recorded, the revocation data being generated based on a media key and device key data and intended for revoking a device key, the device key data being held by reproduction apparatuses classified into N-categories and belonging to the respective categories, the device key being held by a specific reproduction apparatus of the respective categories, the encrypted content being generated by encrypting the content based on the media key, and N being a natural number greater than one.

14. The recording medium according to Claim 13,

wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatuses of a corresponding

category.

15. The recording medium according to Claim 14,

wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key.

16. The recording medium according to Claim 14,

wherein the encrypted content is generated by encrypting the content using a content key, and

on said recording medium, an encrypted content key is recorded, the encrypted content key being generated by encrypting the content key using the media key.

17. The recording medium according to Claim 13,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by the reproduction apparatuses of the corresponding category,

the encrypted content is generated by encrypting the content using a content key, and

on said recording medium, N-pieces of encrypted content keys generated by encrypting the content key using the N-pieces of media keys are recorded.

18. The recording medium according to Claim 13,

wherein on said recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded, the first revocation data being generated based on the media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second

revocation data being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category, and the encrypted content being the content on which an encryption process has been performed based on the media key.

19. A reproduction apparatus which reproduces an encrypted content recorded on a recording medium,

wherein said reproduction apparatuses are classified into N-categories, N being a natural number greater than one,

on the recording medium, at least revocation data and an encrypted content are recorded, the revocation data being generated based on a media key and device key data and intended for revoking a device key, the device key data being held by said reproduction apparatuses of the respective N-categories, the device key being held by a specific reproduction apparatus of the respective categories, and the encrypted content being generated by encrypting the content based on the media key, and

said reproduction apparatus is operable (a) to read out, from the recording medium, revocation data, among the N-pieces of revocation data, which is for the category to which said reproduction apparatus belongs, and the encrypted content, and (b) to decrypt the encrypted content based on the read-out revocation data.

20. The reproduction apparatus according to Claim 19,

wherein each of the N-pieces of revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatuses of a corresponding category, and

said reproduction apparatuses are operable (a) to read out, from the recording medium, the corresponding encrypted media key

data and the encrypted content, (b) to obtain the media key by decrypting the encrypted media key data using the held device key, and (c) to decrypt the encrypted content based on the obtained media key.

21. The reproduction apparatus according to Claim 20,

wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key, and

said reproduction apparatus is operable to generate a decryption key based on the obtained media key, and to decrypt the encrypted content based on the generated decryption key.

22. The reproduction apparatus according to Claim 20,

wherein the encrypted content is generated by encrypting the content using a content key,

on the recording medium, an encrypted content key generated by encrypting the content key using the media key is recorded, and

said reproduction apparatus is operable (a) to read out the encrypted content key from the recording medium, (b) to obtain the content key by decrypting the encrypted content key using the media key, and (c) to decrypt the encrypted content using the obtained content key.

23. The reproduction apparatus according to Claim 19,

wherein each of the N-pieces of revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key data held by the reproduction apparatuses of the corresponding category,

the encrypted content is generated by encrypting the content using a content key,

on the recording medium, N-pieces of encrypted content keys generated by encrypting the content key using the N-pieces of media keys are recorded, and

said reproduction apparatus is operable (a) to read out, from the recording medium, the encrypted media key data for the corresponding category, the encrypted content key for the corresponding category, and the encrypted content, (b) to obtain the media key for the corresponding category by decrypting the encrypted media key data using the held device key, (c) to obtain the content key by decrypting the encrypted content key using the obtained media key for the corresponding category, and (d) to decrypt the encrypted content using the obtained content key.

24. The reproduction apparatus according to Claim 19,

wherein on the recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded, the first revocation data being generated based on the media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category, and the encrypted content being the content on which an encryption process has been performed based on the media key, and

said reproduction apparatus belongs to the second category and is operable to read out, from the recording medium, the second revocation data and the encrypted content, and to decrypt the encrypted content based on the second revocation data.

25. A read-out apparatus included in a reproduction apparatus

which reproduces an encrypted content recorded on a recording medium,

wherein on the recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded, the first revocation data being generated based on a media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data being generated based on the media key and on device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category, and the encrypted content being the content on which an encryption process has been performed based on the media key, and

said read-out apparatus belongs to the second category and is operable (a) to read out, from the recording medium, the first revocation data, the second revocation data, and the encrypted content, (b) to generate intermediate data which is the encrypted data on which a part of a decryption process has been performed, based on the second revocation data, and (c) to output the generated intermediate data and the first revocation data.

26. A decryption apparatus included in a reproduction apparatus which reproduces an encrypted content recorded on a recording medium,

wherein on the recording medium, at least first revocation data, second revocation data, and the encrypted content are recorded, the first revocation data being generated based on a media key and on device key data held by decryption apparatuses of a first category and intended for revoking a device key held by a specific decryption apparatus of the first category, the second revocation data being generated based on the media key and on

device key data held by apparatuses of a second category and intended for revoking a device key held by a specific apparatus of the second category, and the encrypted content being the content on which an encryption process has been performed based on the media key,

read-out apparatuses of the second category are each operable (a) to read out, from the recording medium, the first revocation data, the second revocation data, and the encrypted content, (b) to generate intermediate data which is the encrypted data on which a part of a decryption process has been performed, based on the second revocation data, and (c) to output the generated intermediate data and the first revocation data, and

said decryption apparatus belongs to the first category and is operable to obtain the content by performing a decryption process, based on the first revocation data, on the intermediate data supplied by said read-out apparatus of the second category.

27. A reproduction apparatus which reproduces an encrypted content recorded on a recording medium, said reproduction apparatus comprising: said read-out apparatus according to Claim 25; and said decryption apparatus according to Claim 26.

28. A copyright protection system comprising:

a key generation apparatus operable to generate and record revocation data necessary for encrypting and decrypting a content,

recording apparatuses, each of which is operable to encrypt a content and to record the encrypted content;

a recording medium on which the encrypted content and the revocation data are recorded; and

reproduction apparatuses, each of which is operable to read out and decrypt the encrypted content recorded on said recording medium,

wherein said recording apparatuses and said reproduction apparatuses are classified into N-categories, N being a natural number greater than one,

said key generation apparatus is operable (a) to generate, for the respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key, and (b) to record the N-pieces of revocation data onto said recording medium, the device key data being held by one of said recording apparatuses and said reproduction apparatuses belonging to the respective N-categories, the device key being held by one of a specific recording apparatus and a specific reproduction apparatus of the respective categories,

said recording apparatuses are each operable (a) to read out, from said recording medium, revocation data among the N-pieces of revocation data, which is for the category to which said recording apparatus belongs, (b) to generate the encrypted content by encrypting the content based on the read-out revocation data, and (c) to record the generated encrypted content on said recording medium, and

said reproduction apparatuses are each operable (a) to read out, from said recording medium, revocation data among the N-pieces of revocation data, which is for the category to which said reproduction apparatus belongs, and the encrypted content, and (b) to decrypt the encrypted content based on the read-out revocation data.

29. A key generation apparatus which generates, for respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key, and which records the generated N-pieces of revocation data onto a recording medium, the device key data being held by one of the recording apparatuses and the reproduction apparatuses classified into

N-categories and belonging to the respective categories, the device key being held by one of a specific recording apparatus and a specific reproduction apparatus of the respective categories, and N being a natural number greater than one.

30. A recording apparatus which encrypts a content and records the encrypted content,

wherein said recording apparatus is operable (a) to read out, from a recording medium on which N-pieces of revocation data are recorded, revocation data for a category to which said recording apparatus belongs, (b) to generate an encrypted content by encrypting the content based on the read-out revocation data, and (c) to record the generated encrypted content onto the recording medium, the revocation data being generated based on a media key and device key data and intended for revoking a device key, the device key data being held by one of recording apparatuses and reproduction apparatuses which are classified into N-categories and belonging to the respective categories, the device key being held by one of a specific recording apparatus and a specific reproduction apparatus of the respective categories, and N being a natural number greater than one.

31. A recording method for use in a recording apparatus which encrypts a content and records the encrypted content, said method comprising:

a step of generating, for respective N-categories and based on a media key and device key data, revocation data intended for revoking a device key, the device key data being held by the reproduction apparatuses classified into the N-categories and belonging to the respective N-categories, the device key being held by a specific reproduction apparatus of the respective categories, and N being a natural number greater than one;

an encrypted content generation step of generating the encrypted content by encrypting the content, based on the media key; and

a recording step of recording at least the N-pieces of revocation data and the encrypted content onto the recording medium.

32. A reproduction method for use in a reproduction apparatus which reproduces an encrypted content recorded on a recording medium,

wherein the reproduction apparatuses are classified into N-categories, N being a natural number greater than one,

on the recording medium, at least revocation data and the encrypted content are recorded, the revocation data being generated based on a media key and device key data and intended for revoking a device key, the device key data being held by the reproduction apparatuses of the respective N-categories, the device key being held by a specific reproduction apparatus of the respective categories, and the encrypted content being generated by encrypting the content based on the media key, and

said reproduction method comprises:

a read-out step of reading out, from the recording medium: revocation data among the N-pieces of revocation data, for the category to which the reproduction apparatus belongs; and the encrypted content; and

a decryption step of decrypting the encrypted content based on the revocation data read out in said read-out step.

33. A program for use in a recording apparatus which encrypts a content and records the encrypted content, said program comprising:

a step of generating, for respective N-categories and based

on a media key and device key data, revocation data intended for revoking a device key, the device key data being held by reproduction apparatuses classified into the N-categories and belonging to the respective N-categories, the device key being held by a specific reproduction apparatus of the respective categories, and N being a natural number greater than one;

an encrypted content generation step of generating the encrypted content by encrypting the content, based on the media key;

a recording step of recording at least the N-pieces of revocation data and the encrypted content onto the recording medium.

34. A program for use in a reproduction apparatus which reproduces an encrypted content recorded on a recording medium,

wherein the recording apparatuses are classified into N-categories, N being a natural number greater than one,

on the recording medium, at least revocation data and the encrypted content are recorded, the revocation data being generated based on a media key and device key data and intended for revoking a device key, the device key data being held by the reproduction apparatuses of the respective N-categories, the device key being held by a specific reproduction apparatus of the respective categories, and the encrypted content being generated by encrypting the content based on the media key, and

said program comprises:

a read-out step of reading out, from the recording medium: revocation data among the N-pieces of revocation data, for the category to which the reproduction apparatus belongs; and the encrypted content; and

a decryption step of decrypting the encrypted content based on the revocation data read out in said read-out step.